(54) Title: LOCAL AUTHENTICATION IN A COMMUNICATION SYSTEM
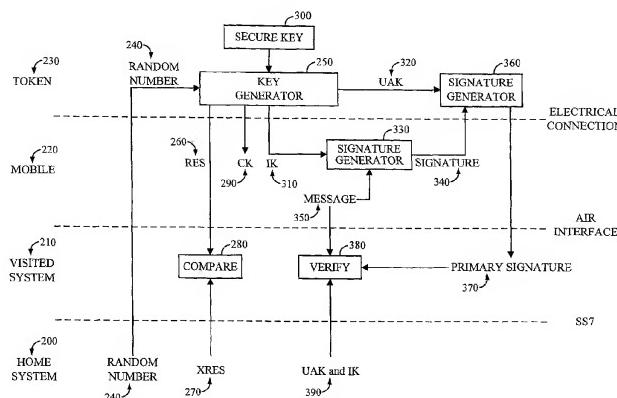
(57) Abstract: Methods and apparatus are presented for providing local authentication of subscribers travelling outside their home
systems. A subscriber identification token (230) provides authentication support by generating a signature (370) based upon a key
that is held secret from a mobile unit (220). A mobile unit (220) that is programmed to wrongfully retain keys from a subscriber
identification token (230) after a subscriber has removed his or her token is prevented from subsequently accessing the subscriber's
account.

WO 02/054663 A3

For two-letter codes and other abbreviations, refer to the "Guidance Notes on Codes and Abbreviations" appearing at the beginning of each regular issue of the PCT Gazette.

INTERNATIONAL SEARCH REPORT

A. CLASSIFICATION OF SUBJECT MATTER
IPC 7   H04Q7/38   H04L9/32   H04L29/06

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)
IPC 7   H04Q   H04L

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practical, search terms used)

EPO-Internal

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category °	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	"Rouges MS_Shell Treat Analysis" 3GPP TSG SA WG3 SECURITY, 'Online! 28 - 30 November 2000, pages 1-17, XP002210348 Sophia Antipolis, France Retrieved from the Internet: <URL:http://www.3gpp.org/ftp/tsg_sa/WG3_Se curity/2000_meetings/TSGS3_16_Sophia_Antip olis/Docs/PDF/S3-000711.pdf> 'retrieved on 2002-08-20!	6-9
A	paragraph '02.2! paragraph '2.4.4! paragraph '05.2! --- -/--	1-5, 10-20

[X] Further documents are listed in the continuation of box C.   [ ] Patent family members are listed in annex.

° Special categories of cited documents :

"A" document defining the general state of the art which is not considered to be of particular relevance

"E" earlier document but published on or after the international filing date

"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)

"O" document referring to an oral disclosure, use, exhibition or other means

"P" document published prior to the international filing date but later than the priority date claimed

"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention

"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone

"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art.

"&" document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
20 August 2002	05/09/2002

Authorized officer

Figiel, B

Form PCT/ISA/210 (second sheet) (July 1992)

C.(Continuation) DOCUMENTS CONSIDERED TO BE RELEVANT		
Category °	Citation of document, with indication,where appropriate, of the relevant passages	Relevant to claim No.
A	ALBERT LEVI, M. UFUK CAGLAYAN: "A Multiple Signature Based Certificate Verification Scheme" BOGAZICI UNIVERSITY, 'Online! XP002210349 Istanbul Retrieved from the Internet: <URL:http://citeseer.nj.nec.com/cache/pape rs/cs/2506/http:zSzzSzmercan.cmpe.boun.edu .trzSz{levizSzbas98.pdf/a-multiple-signatu re-based.pdf> 'retrieved on 2002-08-20! abstract paragraph '0001!	1,10,16, 211

A	"Incorporating UIM into 3G and IMT-2000 Systems" TIA/EIA/IS-808, 'Online! – November 2000 (2000-11) XP002210350 Retrieved from the Internet: <URL:http://www.tiaonline.org/standards/sf g/imt2k/cdma2000/TIA-EIA-IS-808.pdf> 'retrieved on 2002-08-20! page 7 –page 25	1,10,16, 21

A	MEHROTRA A ET AL: "MOBILITY AND SECURITY MANAGEMENT IN THE GSM SYSTEM AND SOME PROPOSED FUTURE IMPROVEMENTS" PROCEEDINGS OF THE IEEE, IEEE. NEW YORK, US, vol. 86, no. 7, July 1998 (1998-07), pages 1480-1497, XP000854168 ISSN: 0018-9219 the whole document	1,10,16, 21